

REMARKS

Applicant respectfully requests reconsideration of this application as amended.

Claims 1 and 3-15 are pending.

By this Amendment, Claim 1 has been amended to recite, *inter alia*, that the information storage means is connected to the information processing means . . . the method comprising using an information processing device for communicating with the portable object, sending from the information processing device to the portable object an order to execute a calculation of a result by applying to the one-way function at least part of said code and entering the result into the implementation of a given operation, the operation being performed successfully only when the portable object is authentic.

Independent Claim 12 has been amended to recite, *inter alia*, information storage means that are connected to the information processing means . . . the information processing means being connected to means for cooperating with an external information processing device distinct from the portable object, so as to receive from an external information processing device an order to execute the calculation.

Independent Claim 14 has been amended to recite that the information storage means is connected to the information processing means and that the device further comprises means for sending the portable object an order so that the portable object determines a result by applying to said one-way function at least part of said code of the portable object, the result entering into the implementation of a given operation, the operation being performed successfully only when the portable object is authentic.

The Office has maintained the outstanding rejections under §§ 102 and 103 in view of Kruse and Anders.

In contrast to the Office's assertions, Applicant respectfully points out that in Kruse, column 2, lines 47-56, "the random number v is generated in the customer card KK and is also forwarded to the customer terminal KT. Dependent on the random number v , a data block P_v is then selected with the assistance of the selection module SEL from the sensitive program parts P." Based on this paragraph, and column 3, lines 14-16 of Kruse which state "an open number of possibilities are conceivable for the selection of a data block P_v from the sensitive program data P with the assistance of the random number v " it is clear that the data block does not define operation steps capable of being executed by the portable object as claimed.

Thus, it is Applicant's understanding that in Kruse the data exchange system comprises a terminal KT in a portable data carrier KK (chip card), in which both the terminal KT and the chip card contain an independent, programmable data memory with an associated control and address circuit. A common authentication algorithm (F) is implemented in a microprocessor in each case in a stored secret cipher, that is identical in each case, and in which a random number (v) is generated with the assistance of a random number generator present in the chip card KK and is transmitted to the terminal KT.

The generated random number (v) selects parts of a program (P) for data flow control from the data memory both in the terminal KT and the chip card KK in each case. An authentication code (PAC_v) is then calculated from the program parts (P_v) in each case with the assistance of the authentication algorithm (F) and of a secret cipher (KPC). The chip card KK verifies the identity of on the one hand the authentication code (PAC_v) determined in the card KK and on the other hand the authentication code (PAC_v) calculated in the terminal KT and transmitted into the chip card.

There is absolutely no teaching or suggestion in Kruse of one code stored in the portable object, the code defining operation steps capable of being executed by the portable object as well as a one-way function as recited in Claim 1. Moreover, Kruse does not teach or suggest sending, from the information processing device, to the portable object, an order to execute a calculation of a result by applying to said one-way function at least part of said code.

Kruse discloses a random number generator in a chip card for initiating the authentication operations. In contradistinction, Claim 1 recites sending from the information processing device to the portable object. Moreover, Kruse does not teach or suggest one code as claimed.

Comparable distinctions can be drawn between Claims 9, 12 and 14 and the Kruse reference. At least based on these distinctions, Applicant respectfully submits that Kruse does not anticipate or render obvious these claims. Since the Anders reference fails to overcome at least the above deficiencies, Applicant respectfully submits the outstanding rejections are untenable and should be withdrawn.

An early Notice of Allowance is respectfully requested.

Should the Examiner believe that any further action is necessary to place this application in better form for allowance, the Examiner is invited to contact Applicant's representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to deposit account number 50-1165 (T2146-907683) any fees under 37 CFR § 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any

extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

EJK:JHV:jab

Miles & Stockbridge P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
(703) 903-9000

By: 

Edward J. Kondracki
Reg. No. 20,604

Jason H. Vick
Reg. No. 45,285

March 21, 2005